

## **CERTIFICATE OF COMPLIANCE**

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification of City of Cartersville, Georgia  
d/b/a Cartersville Fibercom, EB Docket 06-36**

Date Filed: February 5, 2010

Name of municipality covered by this certification: **City of Cartersville, Georgia d/b/a  
Cartersville Fibercom**

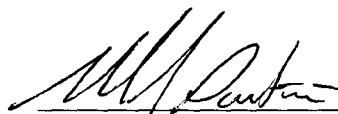
Form 499 Filer ID: 827143

Name of signatory: **Matthew J. Santini**

Title of signatory: **Mayor**

I, Matthew J. Santini, certify that I am mayor and thereby an officer of the **City of Cartersville, Georgia**, a municipality doing business as Cartersville Fibercom ("City") and, acting as an agent of the City, that I have personal knowledge that the City has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the Federal Communications Commission's rules governing use and disclosure of confidential proprietary network information ("CPNI"), as governed by Section 222 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996, and as set forth in Part 64, Subpart U of the of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq.*

The City has not received any customer complaints in the past calendar year concerning the unauthorized release of CPNI, and is not aware of any unauthorized disclosures of CPNI. The City does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. The City therefore has not taken any actions against data brokers, including proceedings instituted or petitions filed by the City at the Georgia Public Service Commission, the court system or at the Commission. The City has established procedures to report any future breaches to the FBI and United States Secret Service, and it has emphasized in its employee training of the need for vigilance in identifying and reporting unusual activity in order to enable the City to continue to take reasonable measures to discover and protect against pretexting and other unauthorized access to CPNI.



Matthew J. Santini

Mayor

City of Cartersville, Georgia

Executed February 4, 2010

## **CPNI Compliance Policies of The City of City of Cartersville, Georgia**

The Fibercom Division of the City of Cartersville, Georgia ("City") has implemented the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.*, including the FCC's new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007).

CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

The City's policy is administered by its Fibercom Division's CPNI Compliance Manager, Lamar Greeson.

### **I. USE, DISCLOSURE OF, AND ACCESS TO CPNI**

The City may use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including to initiate, render, bill and collect for telecommunications services; to protect the rights or property of City, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

The City does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

The City does not use CPNI to market its services. In the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use would be subject to a supervisory review process that shall involve the CPNI Compliance Manager. If such use is approved, the City shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

In accordance with Section 222(b) of the Act, 47 U.S.C. § 222(b), if City receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it will only use such information for such purpose, and would not use such information for its own marketing efforts.

## **II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES**

City will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to City's existing policies that would strengthen protection of CPNI, they should report such information immediately to City's CPNI Compliance Manager so that City may evaluate whether existing policies should be supplemented or changed.

Pursuant to 47 C.F.R. § 64.2010(g), the FCC's authentication requirements set forth in § 64.2010 do not apply to City's telecommunications services customers, because all such customers are business customers who may contact a dedicated account representative, and all have a contract with City that specifically addresses City's protection of CPNI. In any event, City does not disclose Call Detail Information to any inbound telephone caller, does not provide online access to any account that provides access to CPNI, and does not provide CPNI to any visitor to a retail office that has not been properly authenticated.

## **III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT**

Any City employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the City CPNI Compliance Manager, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is City's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate City's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

Nothing in this policy authorizes any employee to violate Georgia law. In the event of an apparent conflict between Georgia law and the FCC's CPNI requirements or the requirements of this policy, the City CPNI Compliance Manager will consult the City's legal counsel.

### **A. Identifying a "Breach"**

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a City employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to City's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. The City's CPNI Compliance Manager will determine whether it is appropriate to update City's CPNI policies or training materials in light of any new information.

#### **B. Notification Procedures**

As soon as practicable, and in no event later than 7 business days upon learning of a breach, the City CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or <http://www.fcc.gov/eb/cpni>) for instructions.

City will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI, except as provided below (a full business day does not count a business day on which the notice was provided). If City receives no response from law enforcement after the 7<sup>th</sup> full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

City will delay notification to customers or the public upon request of the FBI or USSS.

If the City Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; City still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

#### **IV. RECORD RETENTION**

The CPNI Compliance Manager is responsible for assuring that City maintains for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

City maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties, or where third parties were allowed access to CPNI.

Because City does not use CPNI for marketing or for any other purpose for which customer approval is required, it does not have any records to keep regarding supervisory review of marketing; or of sales and marketing campaigns that use CPNI; or of records associated with customers' approval or non-approval to use CPNI, or notification to customers prior to any solicitation for customer approval to use or disclose CPNI.

City will maintain a record of any customer complaints related to their handling of CPNI, and records of City's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that City considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

City will have an officer, as its authorized agent, sign a compliance certificate on an annual basis stating personal knowledge that City has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how City's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Any confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

## **V. TRAINING**

All employees with access to CPNI receive a summary of City's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, City requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel.